AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "CROSS-REFRERNCE TO RELATED APPLICATIONS" in its entirety are substitute the following section therefor:

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of co-pending U.S. Patent Application Serial Number 10/674057 (Docket CNTR.2224) entitled *MICROPROCESSOR APPARATUS AND METHOD FOR PERFORMING BLOCK CIPHER CRYPTOGRAPHIC FUNCTIONS*, having a common assignee and common inventors, and filed on 9/29/2003.

[0001] This application claims the benefit of U.S. Provisional Application No. 60/464394 (Docket CNTR.2222), filed on 4/18/2003, which is herein incorporated by reference for all intents and purposes.

Please delete the section entitled "SUMMARY" in its entirety are substitute the following section therefor:

SUMMARY OF THE INVENTION

[0019] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, ~~an apparatus in a microprocessor is provided for accomplishing cryptographic operations. The apparatus includes translation logic and execution logic. The translation logic receives a cryptographic instruction from a source therefrom, where the cryptographic instruction prescribes one of the cryptographic operations. The translation logic also translates the cryptographic instruction into a sequence of micro instructions specifying sub-operations required to accomplish the one of the cryptographic operations. The execution logic is operatively coupled to the translation logic. The execution logic receives the sequence of micro instructions and performs the sub-operations.~~ an instruction is provided for employment by a device. The instruction directs the device to perform a cryptographic operation. The instruction has and opcode field and a repeat prefix field. The opcode field prescribes that the device accomplish the cryptographic operation as further specified within a control word stored in a memory.

The repeat prefix field is coupled to the opcode field. The repeat prefix field indicates that the cryptographic operation prescribed by the instruction is to be accomplished on a plurality of blocks of input data.

~~[0020] One aspect of the present invention contemplates a microprocessor apparatus for performing cryptographic operations. The microprocessor apparatus has a cryptographic instruction and translation logic. The cryptographic instruction is provided to a microprocessor as part of an instruction flow. The cryptographic instruction prescribes one of the cryptographic operations. The translation logic translates the cryptographic instruction into associated micro instructions that specify sub operations required to accomplish the one of the cryptographic operations.~~

[0021] Another aspect of the present invention provides an apparatus for performing cryptographic operations. The apparatus has a cryptographic instruction that is received by logic within a circuit, where the cryptographic instruction prescribes one of the cryptographic operations. The cryptographic instruction includes an opcode field and a repeat prefix field. The opcode field prescribes that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory. The repeat prefix field is coupled to the opcode field. The repeat prefix field indicates that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data.~~The apparatus includes a cryptographic instruction and execution logic. The cryptographic instruction is received by logic within a processor, wherein said cryptographic instruction prescribes one of the cryptographic operations. The execution logic is coupled to said logic. The execution logic performs the one of the cryptographic operations.~~

~~[0022] A further aspect of the present invention comprehends a method for performing cryptographic operations in a processor. The method includes receiving a cryptographic instruction, where the cryptographic instruction prescribes one of the cryptographic operations; and executing the one of the cryptographic operations.~~